Security Visualization

vi·su·al·i·za·tion *noun*

\ˌvi-zhə-wə-lə-ˈzā-shən, ˌvi-zhə-lə-, ˌvizh-wə-lə-\

1 : formation of mental visual images

2 : the act or process of interpreting in visual terms or of putting into visible form

Still impressed
the visualizatio

Visualization can be
Impressive!

Visualization can
reveal previously
nknown information

can be startling,
p crowds!

Hi! I'm Tim.

Useful and/or impressive?

Useful and/or impressive?

VISUALIZATION FOR SECURITY

- Security work is likely to remain **highly human intensive**, yet the work is becoming increasingly challenging.
- High-volume, multidimensional, heterogeneous, and distributed data streams need to be **analyzed** both in **real time** and **historically**.
- current techniques try to match the needs of security administrators to gain **situational awareness**, correlate and classify security events, and improve their effectiveness by reducing noise in the data.

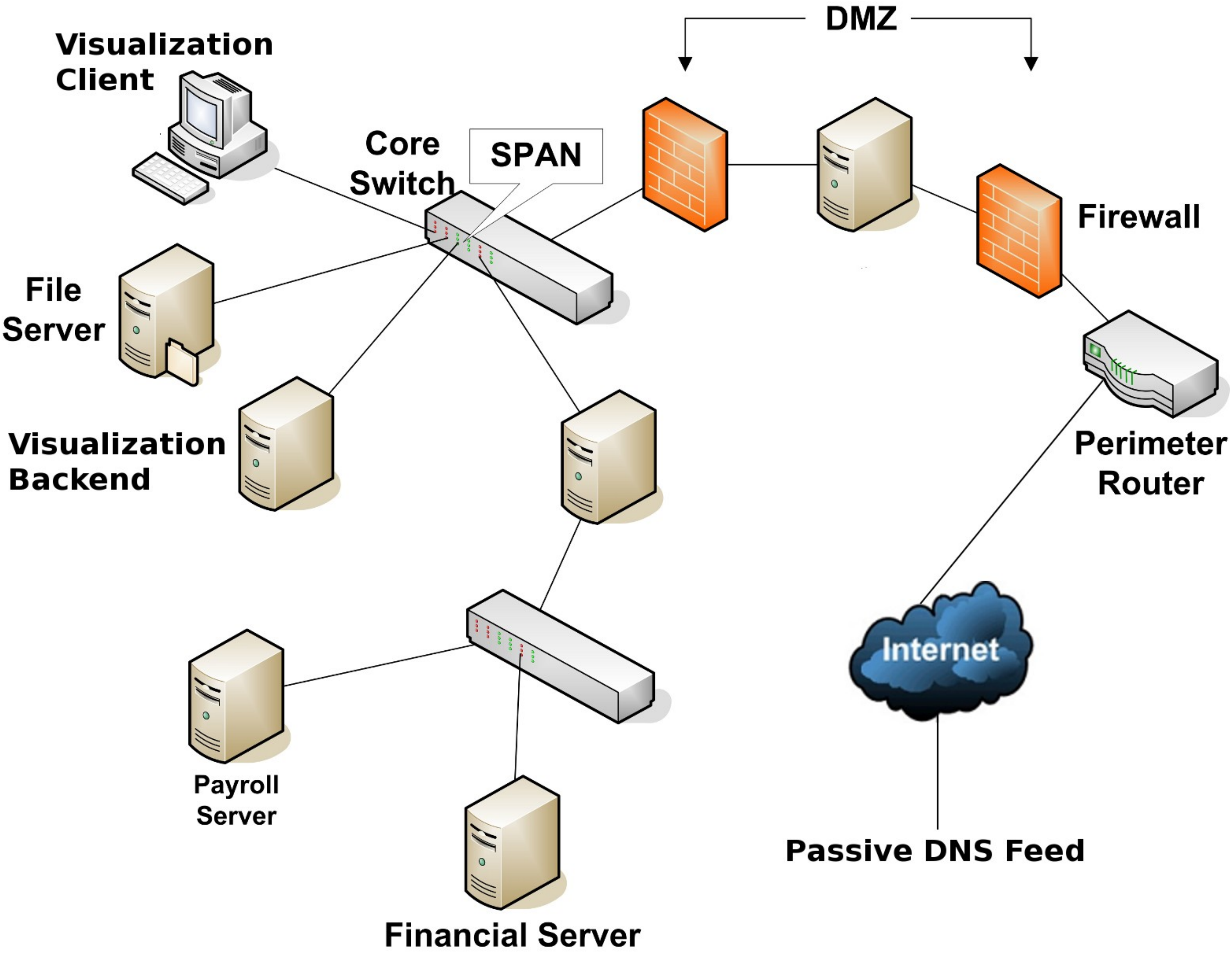
VISUALIZATION FOR SECURITY

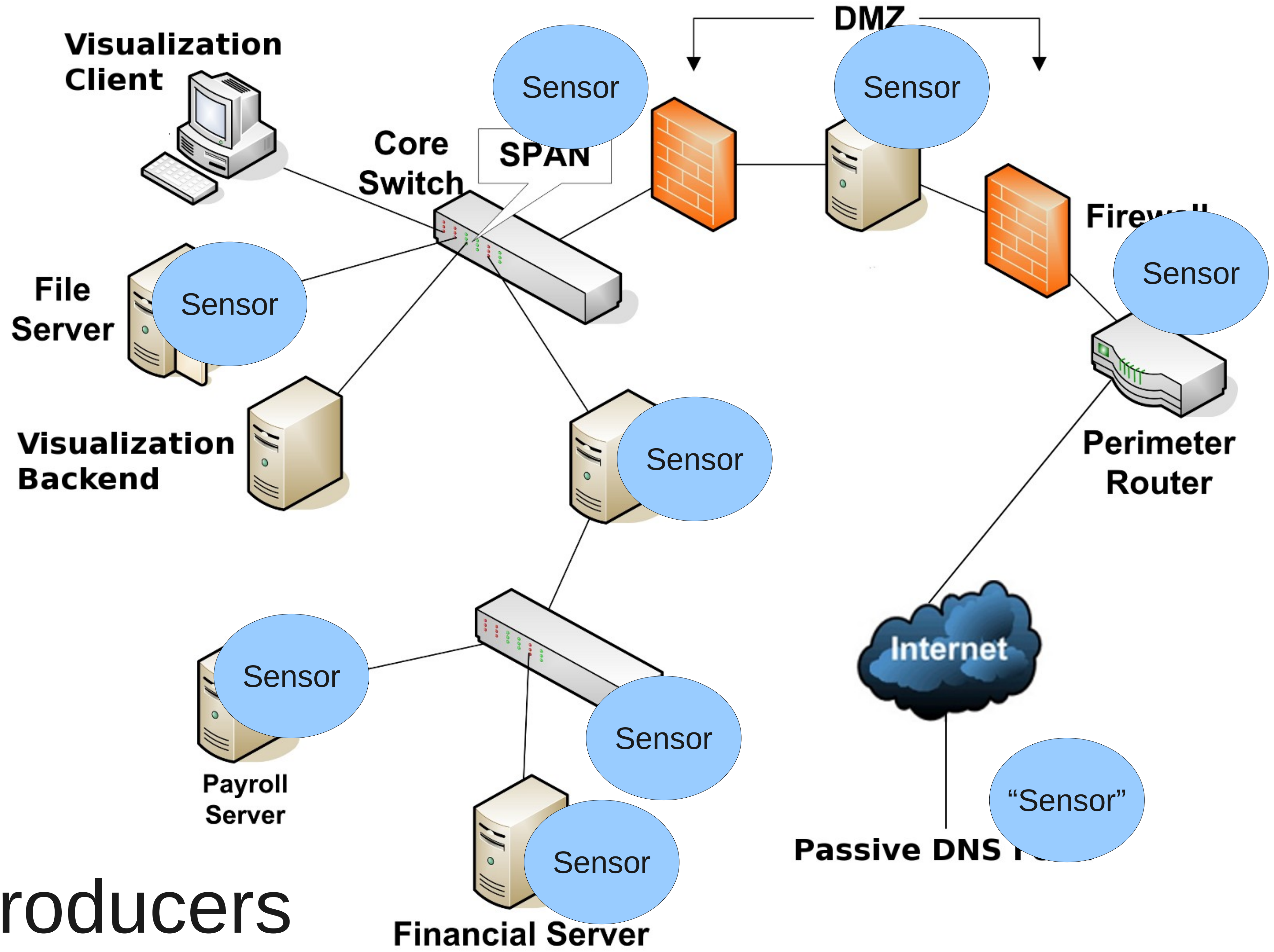
- Security visualization tools are currently **underutilized**.

- Visualization coupled with data mining is likely to **help security administrators make sense** of network flow dynamics, vulnerabilities, intrusion detection alarms, virus propagation, logs, and attacks.

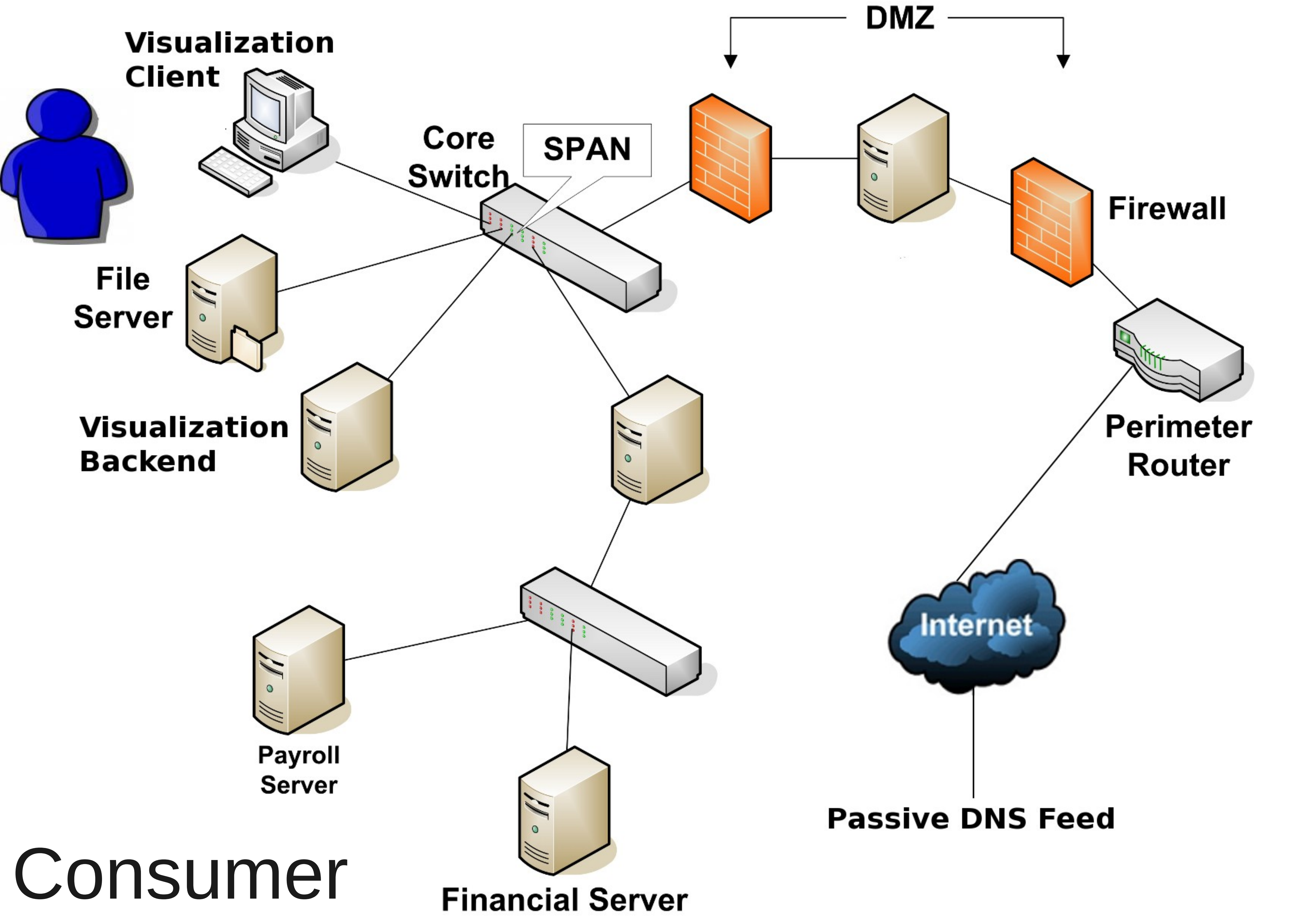
Key features of net viz

- Interactivity: User must be able to interact with the visualization
- Drill-Down capability: User must be able to gain more information if needed
- Conciseness: Must show the state of the entire network in a concise manner


DMZ
Visualization Client
Core Switch
SPAN
Firewall
File Server
Perimeter Router
Visualization Backend
Internet
Payroll Server
Passive DNS Feed
Financial Server


DMZ
Visualization Client
Sensor
Sensor
Core Switch
SPAN
Firewall
Sensor
File Server
Sensor
Perimeter Router
Visualization Backend
Sensor
Internet
Sensor
Payroll Server
Sensor
"Sensor"
Passive DNS
Sensor
Financial Server

Producers


DMZ
Visualization Client
Core Switch
SPAN
Firewall
File Server
Perimeter Router
Visualization Backend
Internet
Payroll Server
Passive DNS Feed
Financial Server

Consumer

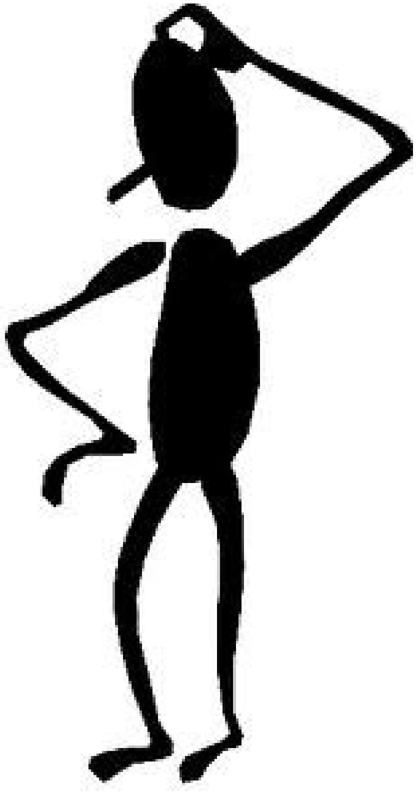
“Typical” setup

- Sensors can be everywhere/anywhere network
  - Logs / Winpcap / libnet / argus / libpcap / snort / etc
- May have external data feeds coming in (poss human)
  - Passive dns, malware, “news”
- Internal / External feeds
  - VPN?
- All feeds go into a central database
- Views are extracted for viz

User Knowledge

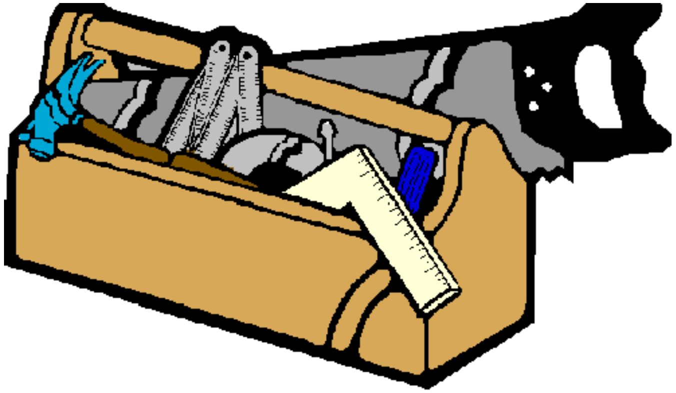
- Even advanced visualizations require extensive knowledge on the part of the user

- The user has to understand what they are looking at



Situational Awareness

- There are lots of tools, most have not received any kind of wide-spread use
- Netwitness
- NvisionIP
- Argus
- Gibson
- Many, many more
- Wireshark
- Etherape
- tnv
- tableau



Tcpdump Argus Packet Processing Comparison

Single TCP connection

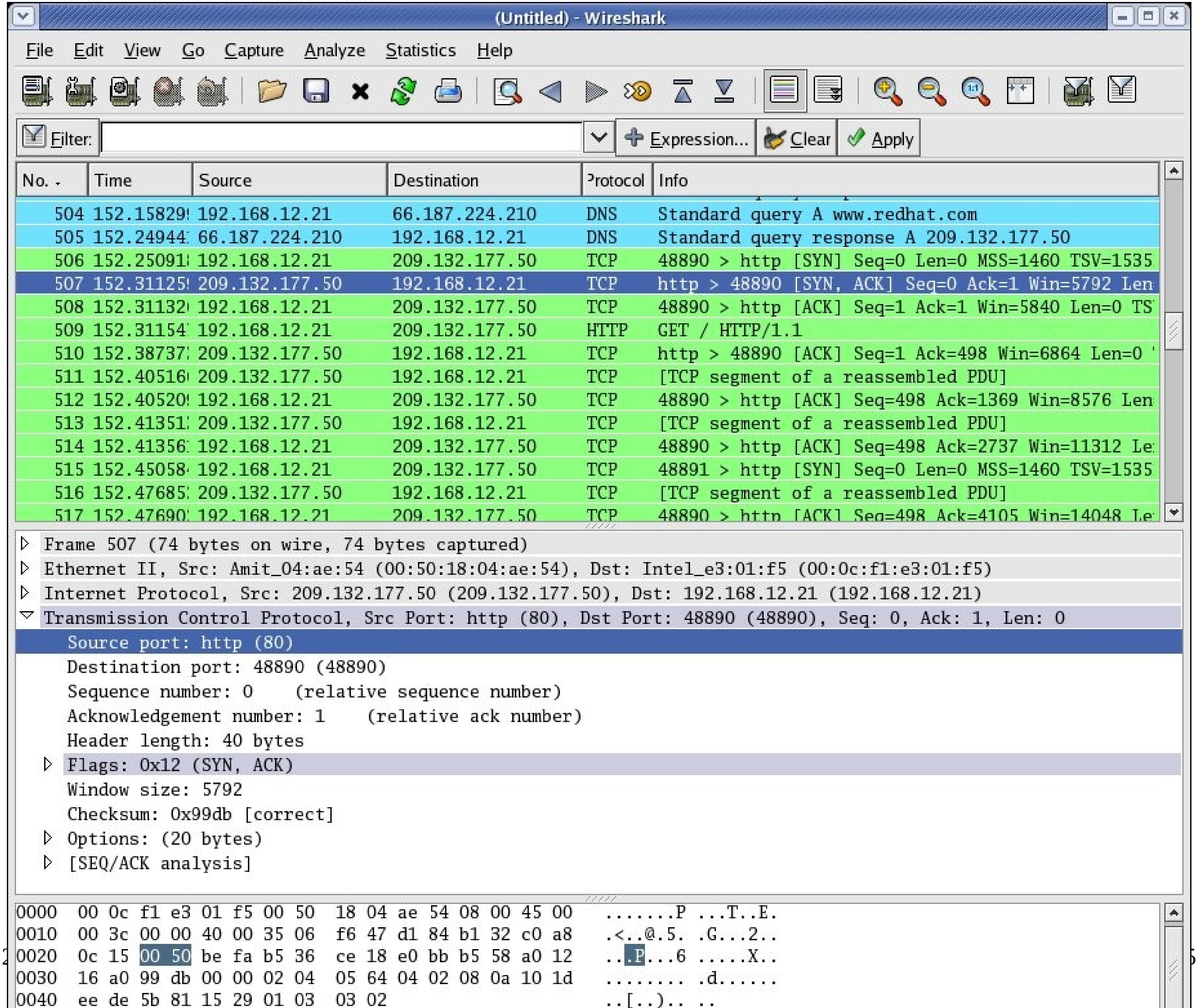
July, 12 2001 09:23:45 - 09:24:14 EDT

```
tcpdump -nr /tmp/tcpdump.out
```

```
                          reading from file /tmp/tcpdump.tcp.out, link-type EN10MB (Ethernet)
                          09:23:45.857732 IP 128.2.24.201.3911 > 207.51.34.153.80: S 2173381702:2173381702(0) win 32120 <mss 1460,sackOK,timestan
Connection Setup          09:23:45.885217 IP 207.51.34.153.80 > 128.2.24.201.3911: S 2130956947:2130956947(0) ack 2173381703 win 17520 <mss 1460
                          09:23:45.885377 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 1 win 32120
                          09:23:45.897456 IP 128.2.24.201.3911 > 207.51.34.153.80: P 1:438(437) ack 1 win 32120
                          09:23:45.943702 IP 207.51.34.153.80 > 128.2.24.201.3911: . 1:1461(1460) ack 438 win 17520
                          09:23:45.944425 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 1461 win 30660
                          09:23:45.945079 IP 207.51.34.153.80 > 128.2.24.201.3911: P 1461:1973(512) ack 438 win 17520
                          09:23:45.953995 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 1973 win 30660
Data Transfer             09:23:45.969729 IP 128.2.24.201.3911 > 207.51.34.153.80: P 438:868(430) ack 1973 win 32120
                          09:23:46.065396 IP 207.51.34.153.80 > 128.2.24.201.3911: P 1973:3084(1111) ack 868 win 17520
                          09:23:46.184010 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 3084 win 31009
                          09:23:46.252909 IP 128.2.24.201.3911 > 207.51.34.153.80: P 868:1307(439) ack 3084 win 32120
                          09:23:46.293312 IP 207.51.34.153.80 > 128.2.24.201.3911: P 3084:4462(1378) ack 1307 win 17520
                          09:23:46.584005 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 4462 win 32120
Server Close Notification 09:24:03.212694 IP 207.51.34.153.80 > 128.2.24.201.3911: F 4462:4462(0) ack 1307 win 17520
                          09:24:03.212829 IP 128.2.24.201.3911 > 207.51.34.153.80: . ack 4463 win 32120
                          09:24:14.271404 IP 128.2.24.201.3911 > 207.51.34.153.80: P 1307:1743(436) ack 4463 win 32120
                          09:24:14.271704 IP 128.2.24.201.3911 > 207.51.34.153.80: F 1743:1743(0) ack 4463 win 32120
Client Close Completion   09:24:14.297823 IP 207.51.34.153.80 > 128.2.24.201.3911: R 2130961410:2130961410(0) win 0
                          09:24:14.298930 IP 207.51.34.153.80 > 128.2.24.201.3911: R 2130961410:2130961410(0) win 0
```

```
argus -r /tmp/tcpdump.out -w - | ra -s +1dur +tcprtt
```

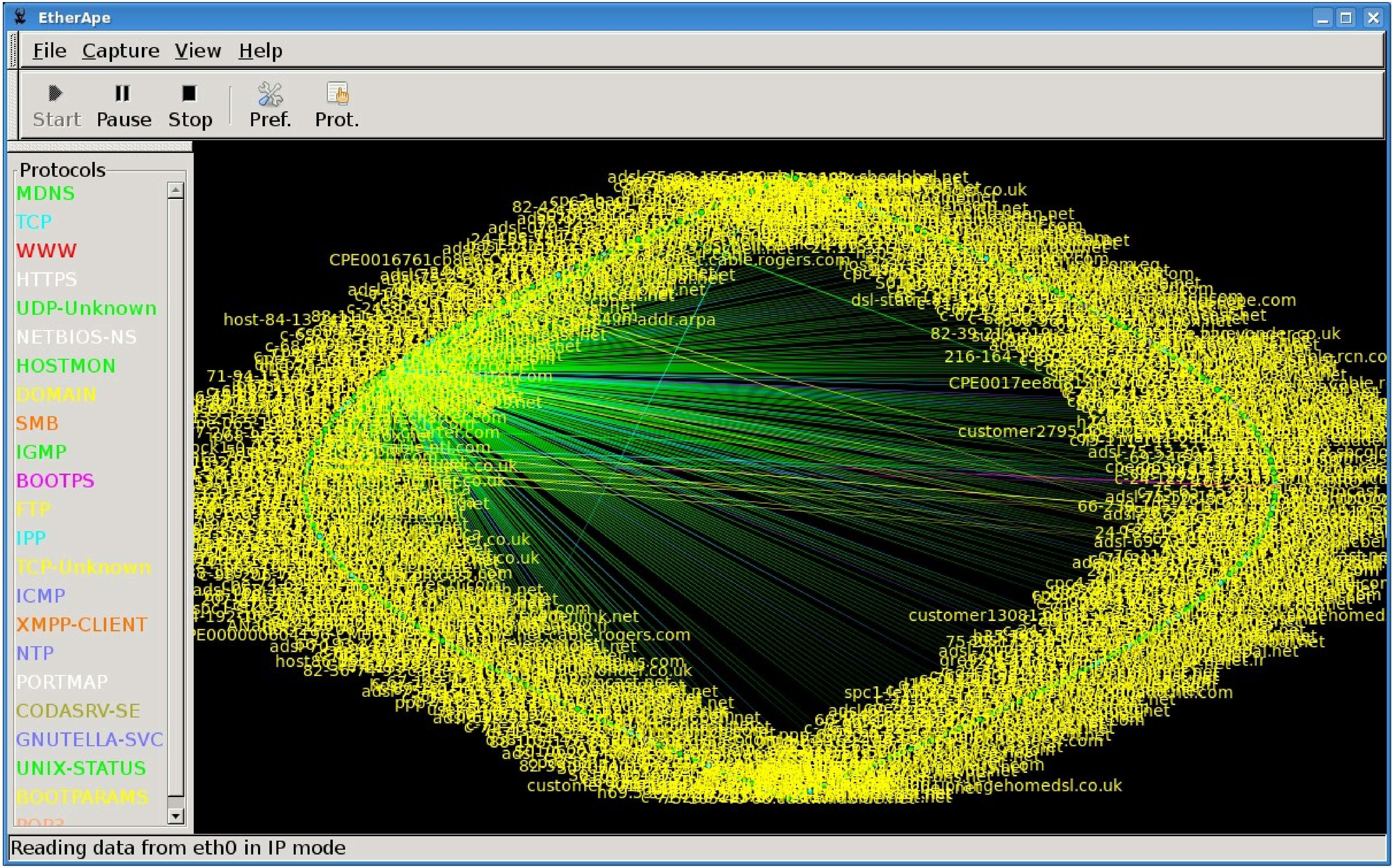
```
                 StartTime        Dur      Flgs  Proto          SrcAddr   Sport    Dir          DstAddr   Dport  SrcPkts  DstPkts     SrcBy
2001/07/12.09:23:45.857732   0.726273  e           tcp     128.2.24.201.3911        ->     207.51.34.153.http         9        5         1
2001/07/12.09:24:03.212694   0.000135  e           tcp     128.2.24.201.3911        ->     207.51.34.153.http         1        1
2001/07/12.09:24:14.271404   0.027526  e           tcp     128.2.24.201.3911        ->     207.51.34.153.http         2        2
```



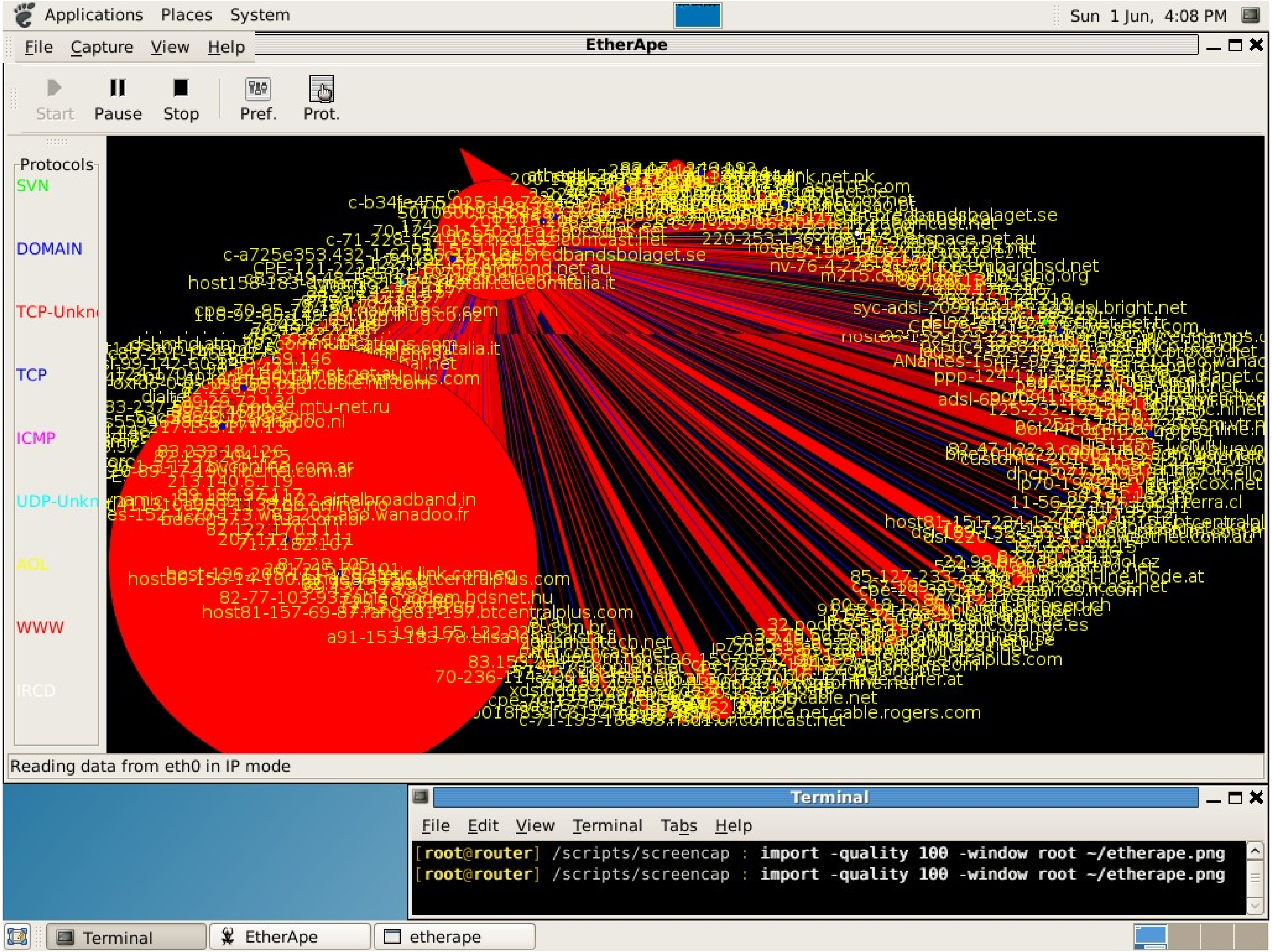
```
No. -  Time       Source           Destination      Protocol Info
  504  152.15829! 192.168.12.21    66.187.224.210   DNS      Standard query A www.redhat.com
  505  152.24944: 66.187.224.210   192.168.12.21    DNS      Standard query response A 209.132.177.50
  506  152.25091! 192.168.12.21    209.132.177.50   TCP      48890 > http [SYN] Seq=0 Len=0 MSS=1460 TSV=1535
  507  152.31125! 209.132.177.50   192.168.12.21    TCP      http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len
  508  152.31132! 192.168.12.21    209.132.177.50   TCP      48890 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TS
  509  152.31154' 192.168.12.21    209.132.177.50   HTTP     GET / HTTP/1.1
  510  152.38737: 209.132.177.50   192.168.12.21    TCP      http > 48890 [ACK] Seq=1 Ack=498 Win=6864 Len=0 '
  511  152.40516! 209.132.177.50   192.168.12.21    TCP      [TCP segment of a reassembled PDU]
  512  152.40520! 192.168.12.21    209.132.177.50   TCP      48890 > http [ACK] Seq=498 Ack=1369 Win=8576 Len
  513  152.41351: 209.132.177.50   192.168.12.21    TCP      [TCP segment of a reassembled PDU]
  514  152.41356: 192.168.12.21    209.132.177.50   TCP      48890 > http [ACK] Seq=498 Ack=2737 Win=11312 Le
  515  152.45058! 192.168.12.21    209.132.177.50   TCP      48891 > http [SYN] Seq=0 Len=0 MSS=1460 TSV=1535
  516  152.47685: 209.132.177.50   192.168.12.21    TCP      [TCP segment of a reassembled PDU]
  517  152.47690: 192.168.12.21    209.132.177.50   TCP      48890 > http [ACK] Seq=498 Ack=4105 Win=14048 Le
```

```
▷ Frame 507 (74 bytes on wire, 74 bytes captured)
▷ Ethernet II, Src: Amit_04:ae:54 (00:50:18:04:ae:54), Dst: Intel_e3:01:f5 (00:0c:f1:e3:01:f5)
▷ Internet Protocol, Src: 209.132.177.50 (209.132.177.50), Dst: 192.168.12.21 (192.168.12.21)
▽ Transmission Control Protocol, Src Port: http (80), Dst Port: 48890 (48890), Seq: 0, Ack: 1, Len: 0
     Source port: http (80)
     Destination port: 48890 (48890)
     Sequence number: 0    (relative sequence number)
     Acknowledgement number: 1    (relative ack number)
     Header length: 40 bytes
   ▷ Flags: 0x12 (SYN, ACK)
     Window size: 5792
     Checksum: 0x99db [correct]
   ▷ Options: (20 bytes)
   ▷ [SEQ/ACK analysis]
```

```
0000  00 0c f1 e3 01 f5 00 50  18 04 ae 54 08 00 45 00   .......P ...T..E.
0010  00 3c 00 00 40 00 35 06  f6 47 d1 84 b1 32 c0 a8   .<..@.5. .G...2..
0020  0c 15 00 50 be fa b5 36  ce 18 e0 bb b5 58 a0 12   ...P...6 .....X..
0030  16 a0 99 db 00 00 02 04  05 64 04 02 08 0a 10 1d   ........ .d......
0040  ee de 5b 81 15 29 01 03  03 02                     ..[..).. ..
```

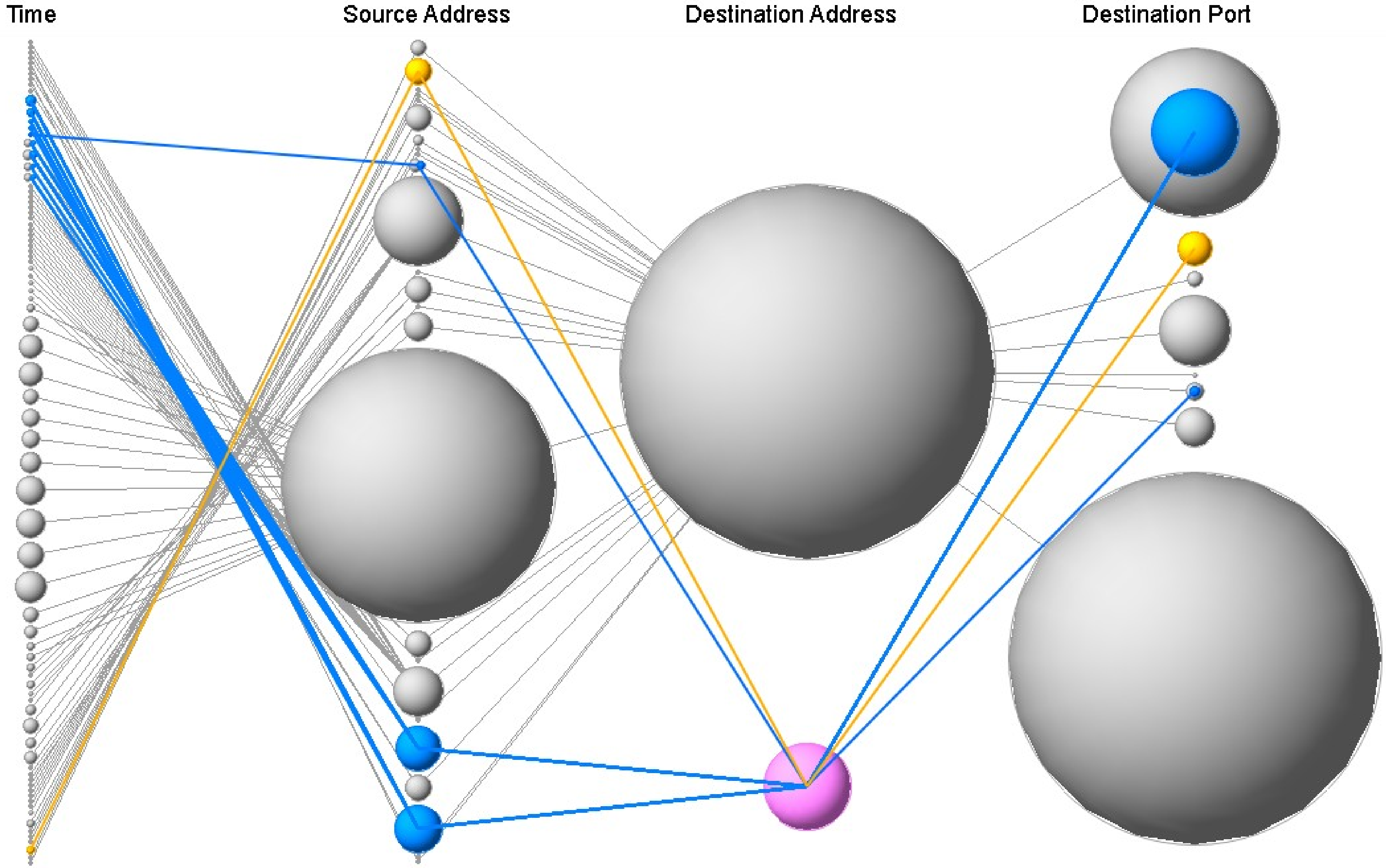


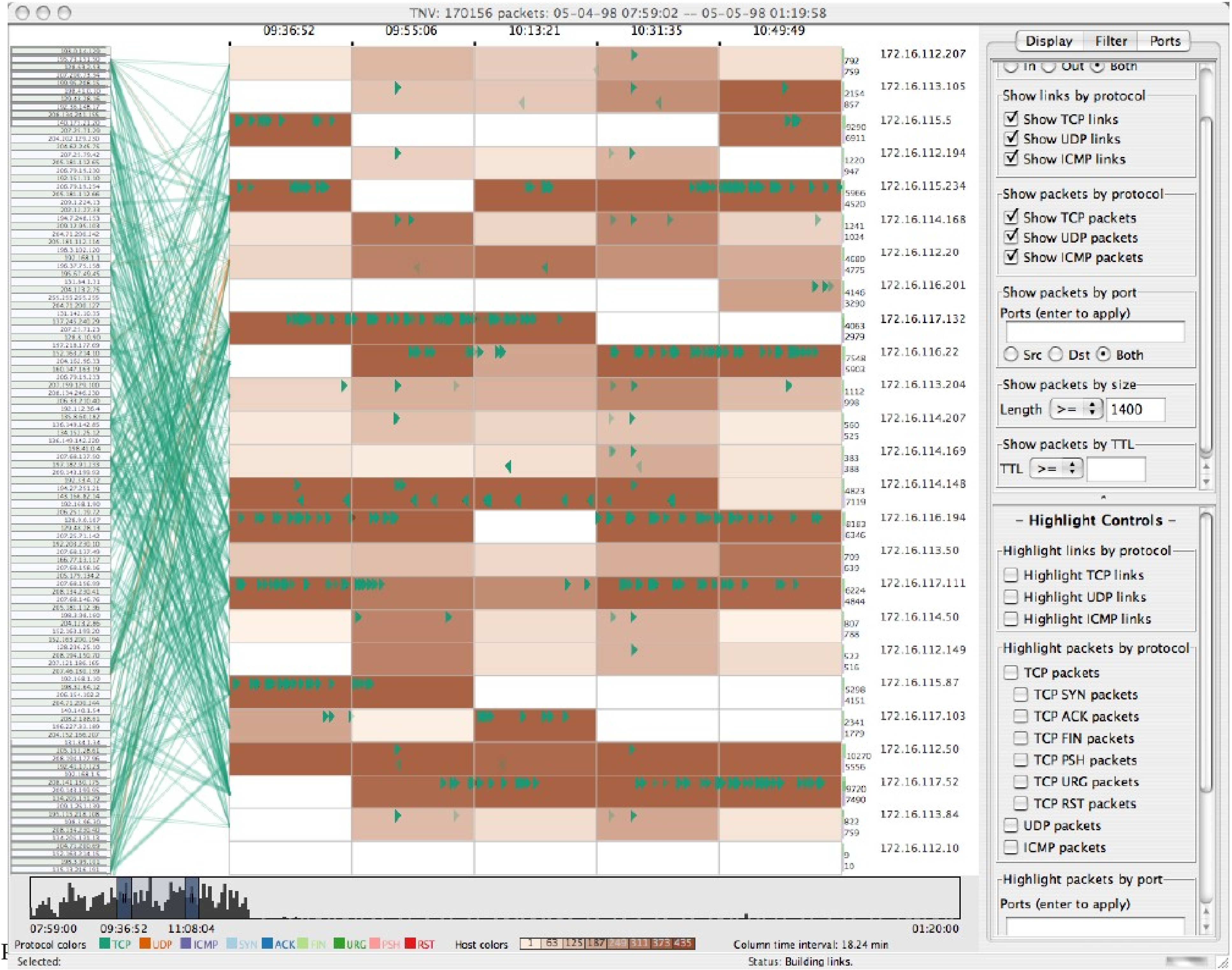
Reading data from eth0 in IP mode



Reading data from eth0 in IP mode

```
[root@router] /scripts/screencap : import -quality 100 -window root ~/etherape.png
[root@router] /scripts/screencap : import -quality 100 -window root ~/etherape.png
```


Time
Source Address
Destination Address
Destination Port



TNV: 170156 packets: 05-04-98 07:59:02 -- 05-05-98 01:19:58

Display | Filter | Ports

○ In ○ Out ● Both

Show links by protocol
☑ Show TCP links
☑ Show UDP links
☑ Show ICMP links

Show packets by protocol
☑ Show TCP packets
☑ Show UDP packets
☑ Show ICMP packets

Show packets by port
Ports (enter to apply)
○ Src ○ Dst ● Both

Show packets by size
Length >= 1400

Show packets by TTL
TTL >=

- Highlight Controls -

Highlight links by protocol
□ Highlight TCP links
□ Highlight UDP links
□ Highlight ICMP links

Highlight packets by protocol
□ TCP packets
□ TCP SYN packets
□ TCP ACK packets
□ TCP FIN packets
□ TCP PSH packets
□ TCP URG packets
□ TCP RST packets
□ UDP packets
□ ICMP packets

Highlight packets by port
Ports (enter to apply)

Protocol colors 🟩 TCP 🟧 UDP 🟪 ICMP 🟦 SYN 🟦 ACK 🟩 FIN 🟩 URG 🟥 PSH 🟥 RST

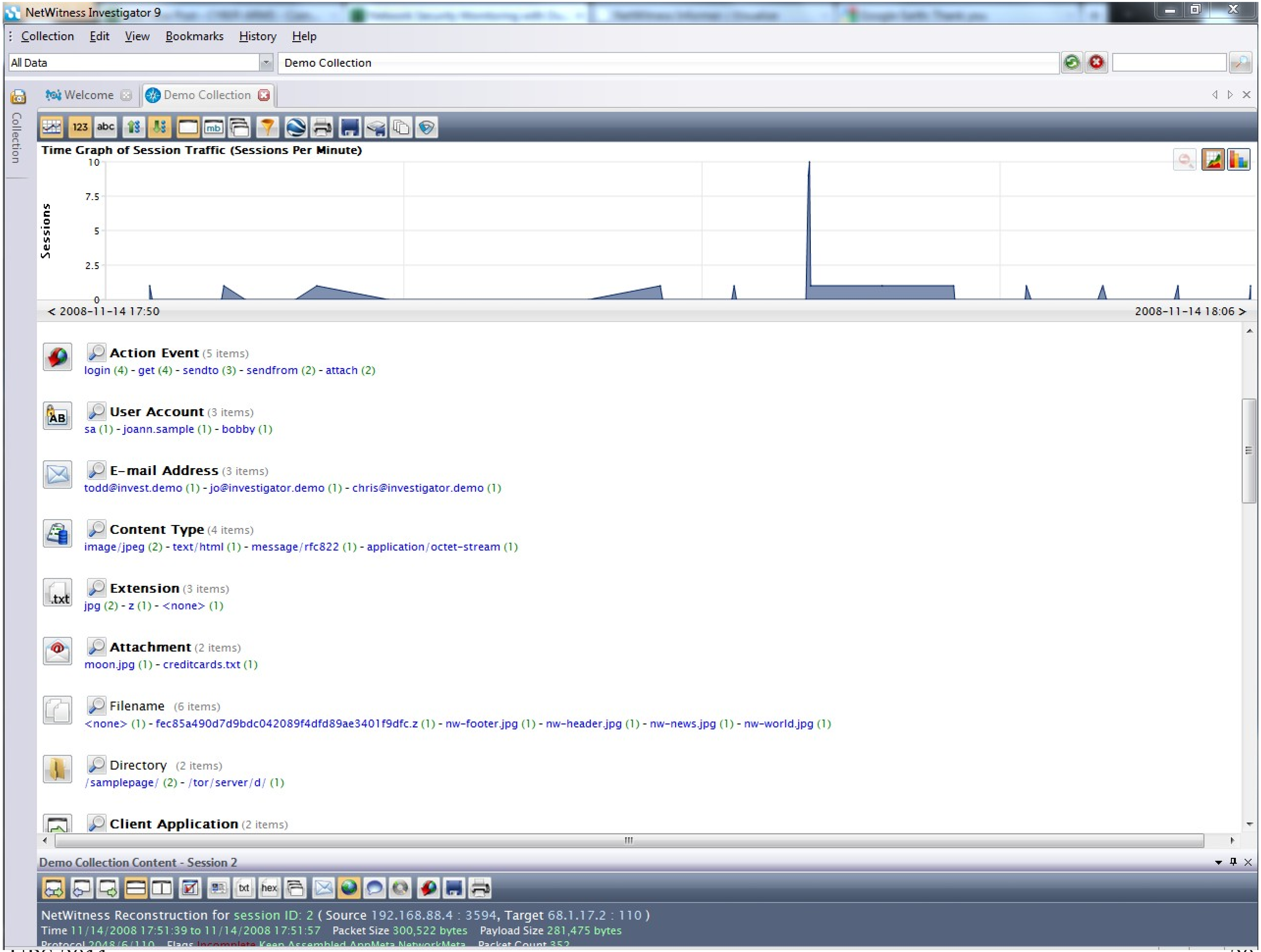
Host colors 1 63 125 187 249 311 373 435

Column time interval: 18.24 min

Selected:

Status: Building links.

UI



Action Event (5 items)
login (4) - get (4) - sendto (3) - sendfrom (2) - attach (2)

User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)

E-mail Address (3 items)
todd@invest.demo (1) - jo@investigator.demo (1) - chris@investigator.demo (1)

Content Type (4 items)
image/jpeg (2) - text/html (1) - message/rfc822 (1) - application/octet-stream (1)

Extension (3 items)
jpg (2) - z (1) - <none> (1)

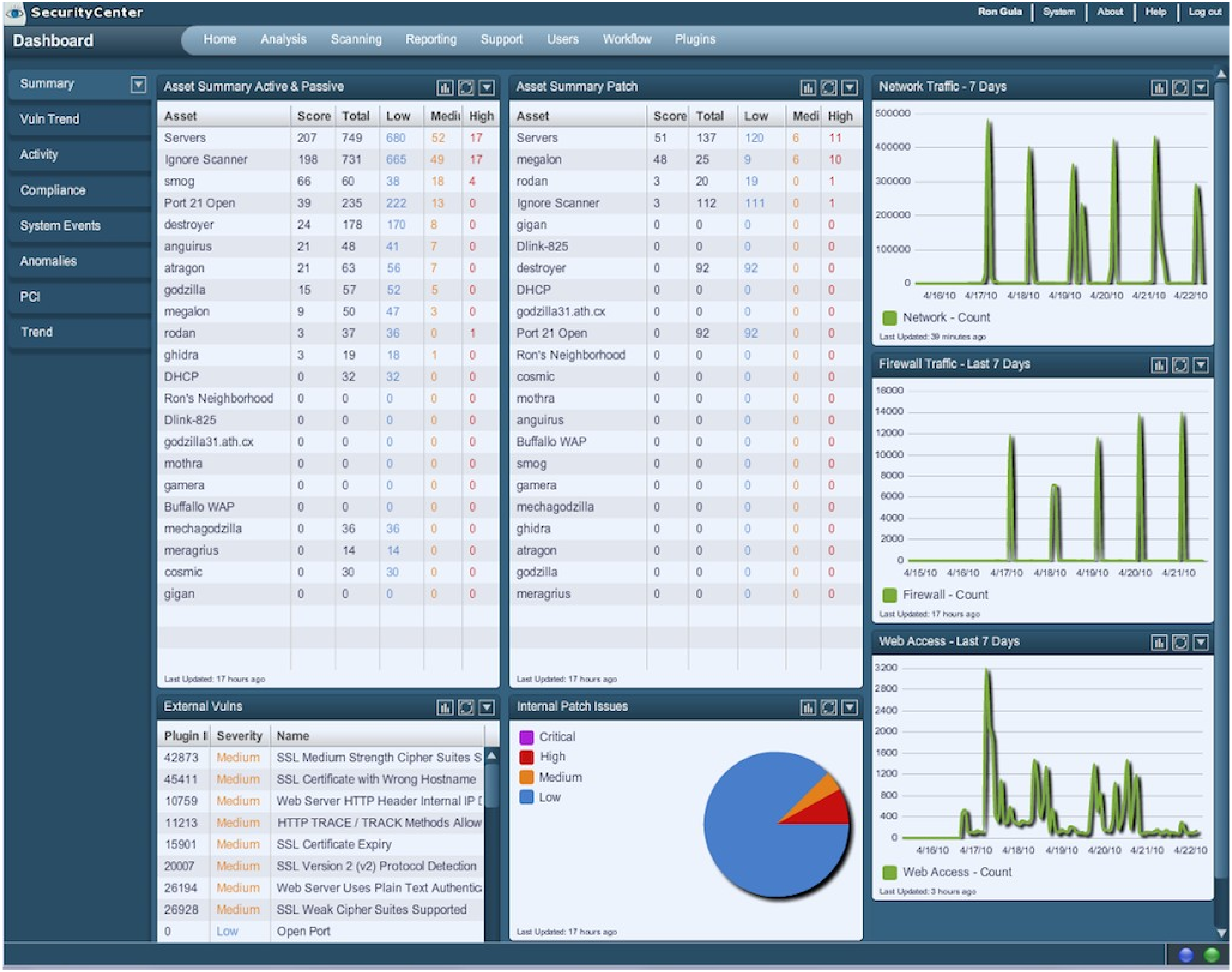
Attachment (2 items)
moon.jpg (1) - creditcards.txt (1)

Filename (6 items)
<none> (1) - fec85a490d7d9bdc042089f4dfd89ae3401f9dfc.z (1) - nw-footer.jpg (1) - nw-header.jpg (1) - nw-news.jpg (1) - nw-world.jpg (1)

Directory (2 items)
/samplepage/ (2) - /tor/server/d/ (1)

Client Application (2 items)

NetWitness Reconstruction for session ID: 2 (Source 192.168.88.4 : 3594, Target 68.1.17.2 : 110)
Time 11/14/2008 17:51:39 to 11/14/2008 17:51:57 Packet Size 300,522 bytes Payload Size 281,475 bytes
Protocol 2048/6/110 Flags Incomplete Keep Assembled AppMeta NetworkMeta Packet Count 352



Asset Summary Active & Passive

Asset	Score	Total	Low	Medi	High
Servers	207	749	680	52	17
Ignore Scanner	198	731	665	49	17
smog	66	60	38	18	4
Port 21 Open	39	235	222	13	0
destroyer	24	178	170	8	0
anguirus	21	48	41	7	0
atragon	21	63	56	7	0
godzilla	15	57	52	5	0
megalon	9	50	47	3	0
rodan	3	37	36	0	1
ghidra	3	19	18	1	0
DHCP	0	32	32	0	0
Ron's Neighborhood	0	0	0	0	0
Dlink-825	0	0	0	0	0
godzilla31.ath.cx	0	0	0	0	0
mothra	0	0	0	0	0
gamera	0	0	0	0	0
Buffallo WAP	0	0	0	0	0
mechagodzilla	0	36	36	0	0
meragrius	0	14	14	0	0
cosmic	0	30	30	0	0
gigan	0	0	0	0	0

Last Updated: 17 hours ago

Asset Summary Patch

Asset	Score	Total	Low	Medi	High
Servers	51	137	120	6	11
megalon	48	25	9	6	10
rodan	3	20	19	0	1
Ignore Scanner	3	112	111	0	1
gigan	0	0	0	0	0
Dlink-825	0	0	0	0	0
destroyer	0	92	92	0	0
DHCP	0	0	0	0	0
godzilla31.ath.cx	0	0	0	0	0
Port 21 Open	0	92	92	0	0
Ron's Neighborhood	0	0	0	0	0
cosmic	0	0	0	0	0
mothra	0	0	0	0	0
anguirus	0	0	0	0	0
Buffallo WAP	0	0	0	0	0
smog	0	0	0	0	0
gamera	0	0	0	0	0
mechagodzilla	0	0	0	0	0
ghidra	0	0	0	0	0
atragon	0	0	0	0	0
godzilla	0	0	0	0	0
meragrius	0	0	0	0	0

Last Updated: 17 hours ago

Network Traffic - 7 Days

Last Updated: 39 minutes ago

Firewall Traffic - Last 7 Days

Last Updated: 17 hours ago

Web Access - Last 7 Days

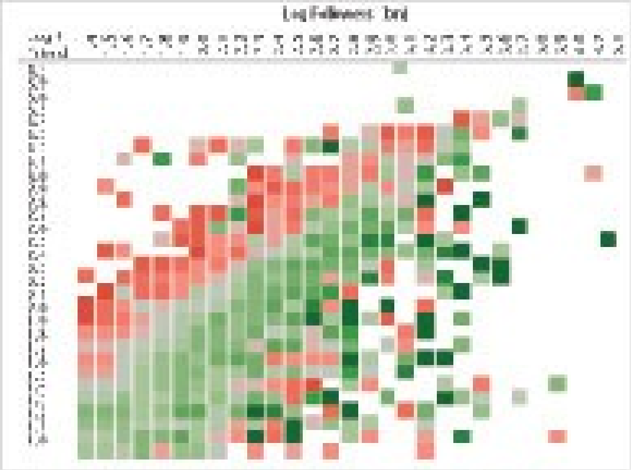
Last Updated: 3 hours ago

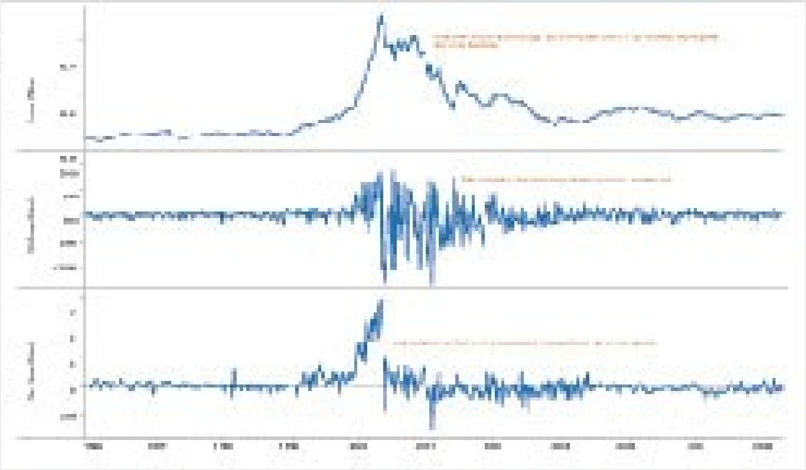
External Vulns

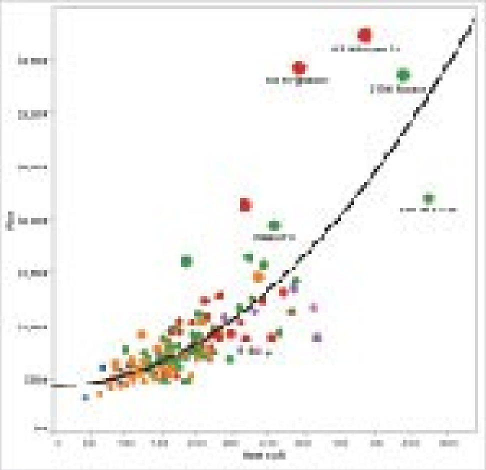
Plugin I	Severity	Name
42873	Medium	SSL Medium Strength Cipher Suites S
45411	Medium	SSL Certificate with Wrong Hostname
10759	Medium	Web Server HTTP Header Internal IP [
11213	Medium	HTTP TRACE / TRACK Methods Allow
15901	Medium	SSL Certificate Expiry
20007	Medium	SSL Version 2 (v2) Protocol Detection
26194	Medium	Web Server Uses Plain Text Authentic
26928	Medium	SSL Weak Cipher Suites Supported
0	Low	Open Port

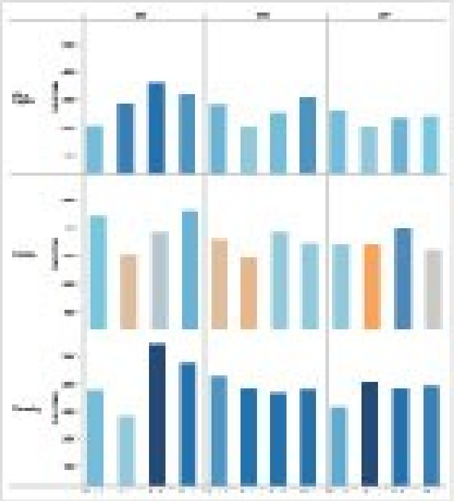
Internal Patch Issues

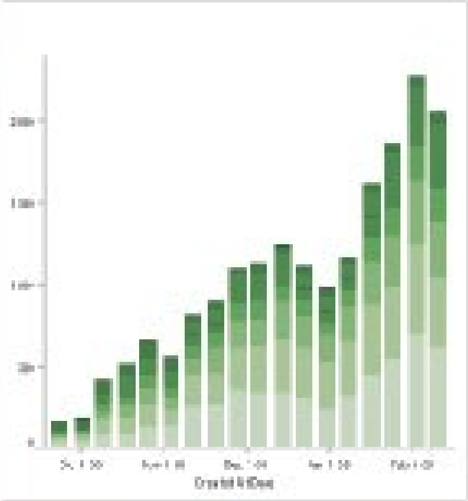
Last Updated: 17 hours ago

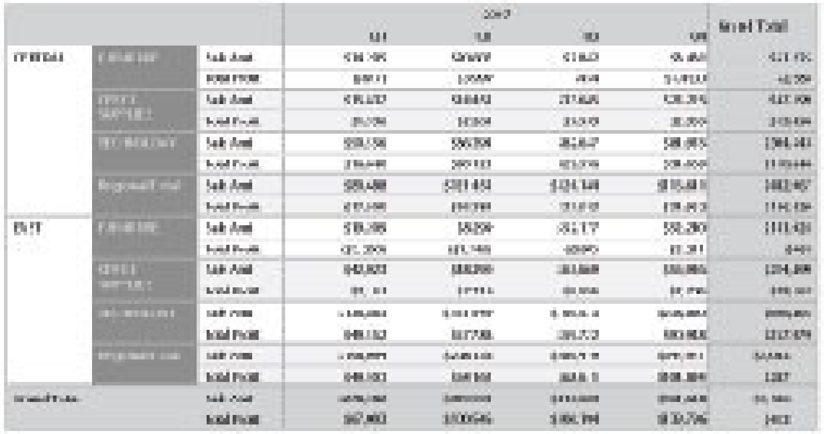




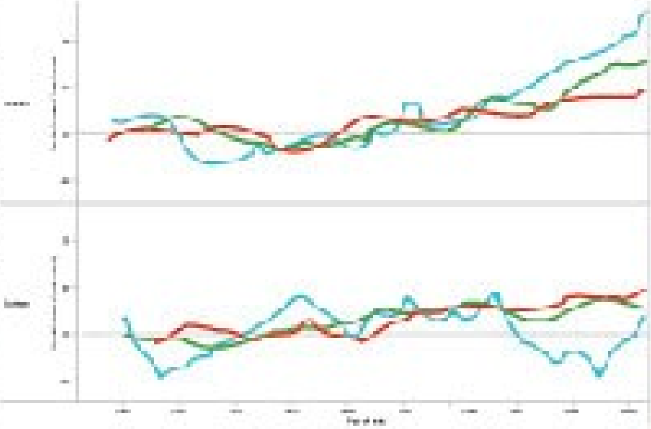


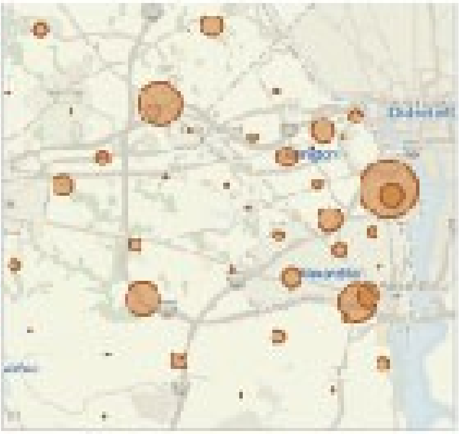






			2007				Grand Total
			Q1	Q2	Q3	Q4	
CENTRAL	FURNITURE	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	OFFICE SUPPLIES	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	TECHNOLOGY	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	Regional Total	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
EAST	FURNITURE	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	OFFICE SUPPLIES	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	TECHNOLOGY	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	Regional Total	Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Grand Total		Sale Amt	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Total Profit	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]



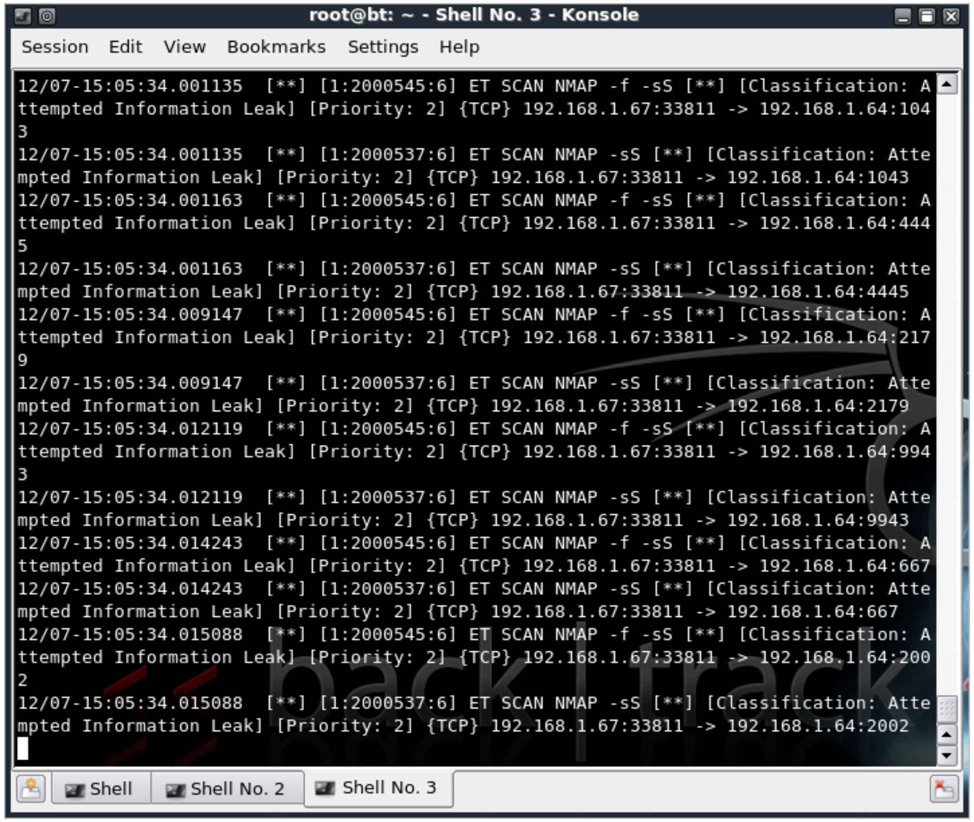


REPORT CONFOR M: IDEOLO- GUE
REGS: INITIATE: OVERDI VE
STATUS REPORT CONFOR M: IDEOLO
NOMINA TE: 00378

Viz is better than no viz

- Studies continuously show that visual interfaces consistently out perform text based interfaces

- So why do administrators forgo viz in favor of this:



```
12/07-15:05:34.001135  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:104
3
12/07-15:05:34.001135  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:1043
12/07-15:05:34.001163  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:444
5
12/07-15:05:34.001163  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:4445
12/07-15:05:34.009147  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:217
9
12/07-15:05:34.009147  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:2179
12/07-15:05:34.012119  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:994
3
12/07-15:05:34.012119  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:9943
12/07-15:05:34.014243  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:667
12/07-15:05:34.014243  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:667
12/07-15:05:34.015088  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:200
2
12/07-15:05:34.015088  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:2002
```

Why don't Admins adopt viz?

- Resistant to change – and text based is the incumbent
- Like their own tools (and text-based is easier to develop)
  - “i know how my own tool works”
  - “i can adapt my own tool to do new things”
  - Using a pre-packaged tool gives an attacker a known quantity to beat

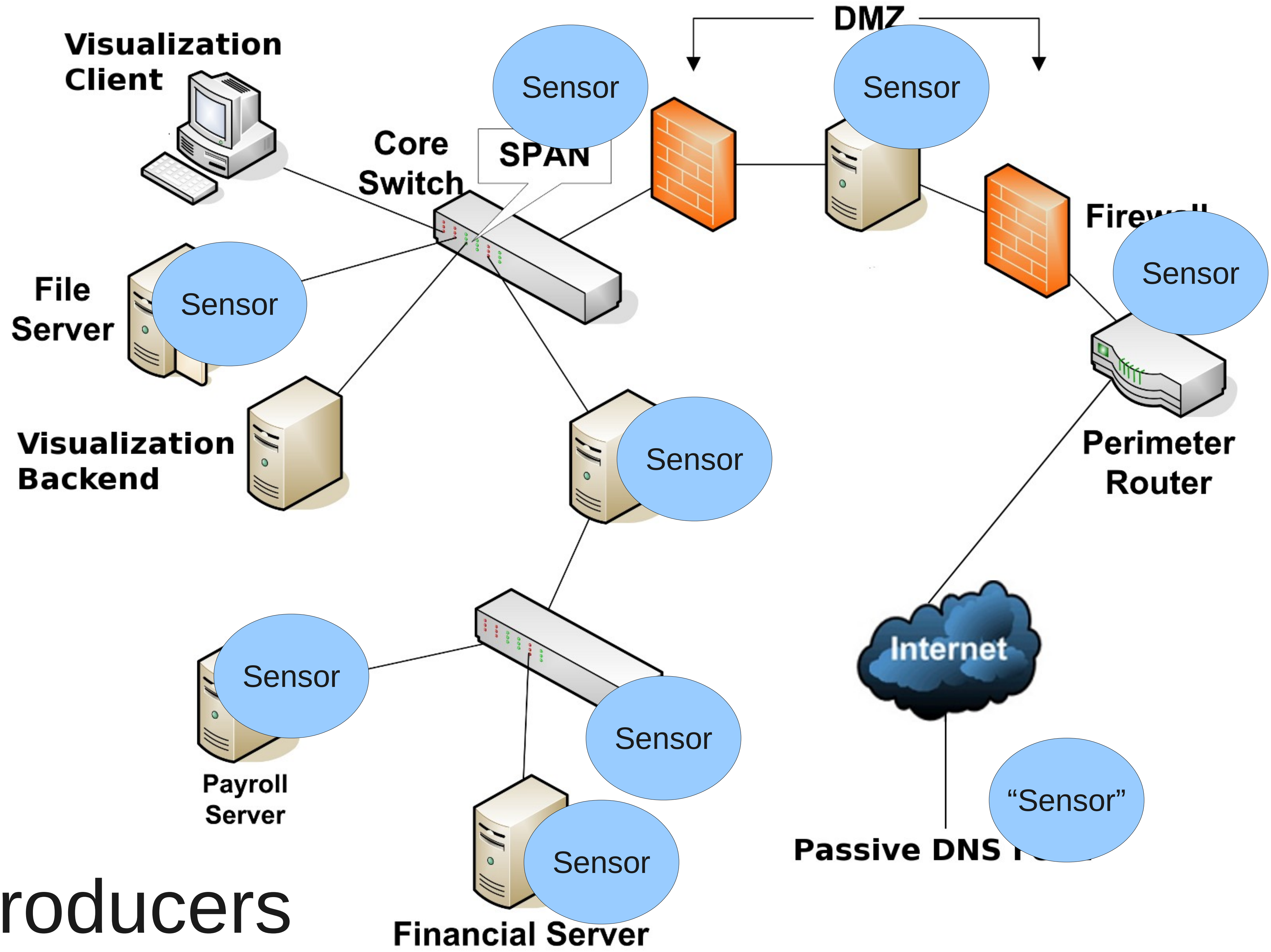
Trust / reliability

Support / extendability / adaptability

security

Weakest link

- As with many security discussions, the viz system is only as strong as it's weakest link
- Successful attacks at any layer can cause information to eventually be misrepresented to the user (the decision maker)


DMZ
Visualization Client
Sensor
Sensor
Core Switch
SPAN
Firewall
Sensor
File Server
Sensor
Perimeter Router
Visualization Backend
Sensor
Internet
Sensor
Payroll Server
Sensor
"Sensor"
Passive DNS
Sensor
Financial Server

Producers

Human perception

- Glass is half ________
- How to lie with charts / stats (Huff, 1954)
- Mislead audiences with results
  - Omit information like 32 vs 64 bit
  - Project results onto multiple systems

  Globus & Bailey
- “Lying” with visualization
  - Claim generality but only test on a single dataset
  - Alter the color map slightly across the graph
  - Don't compare to other viz systems

  Rogowitz

Human ability

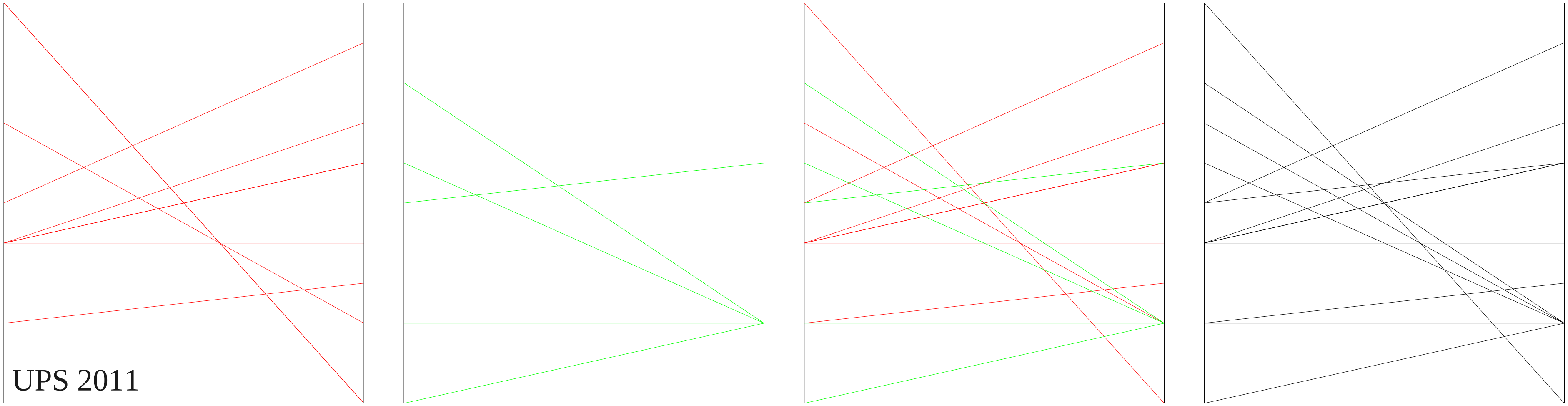
WARNING:

If you have epilepsy or have had seizures or other unusual reactions to flashing lights or patterns, consult a doctor before operating this security visualization tool.

- How many colors can a human differentiate?
- How fast can a human process information?
  - Screen density, “refresh rate,” duration

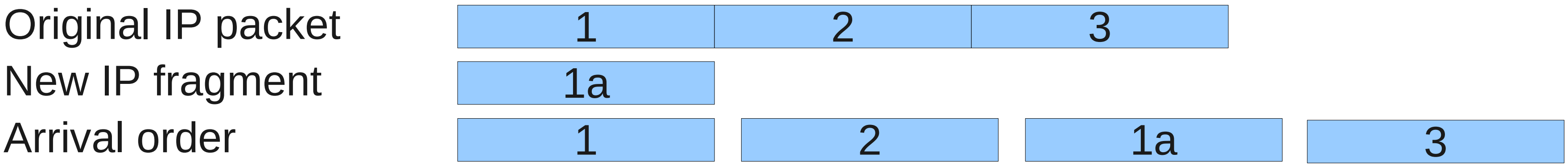
Attacks that target the viz system

- Assuming the attacker know the analyst on duty is red-green color blind
- ICMP is visualized as red and tcp is visualized as green
- An ICMP attack launched during this shift may go unobserved



Attacks that target the viz system

- Tools can only parse what they “understand”
- Attackers specifically abuse protocols, bugs, overlap, etc
- Consider the TCP/IP stack
  - Difference OSes implement it differently
  - IP Fragments are supposed to be contiguous, but what if they are not?
  - The software stack on one OS may recreate the resulting IP datagram differently than on another OS



Original IP packet 1 2 3

New IP fragment 1a

Arrival order 1 2 1a 3

Arms Race

- *Snort* is open source
- Snort rules are open source
- *Snot* uses the rules as input to create fake attacks creating numerous false positives
  - Snort has snot detection rules
    - Snot has randomization features to circumvent snort's snot detection rules

Not quite there yet

Questions?

Further reading

- UPS class recommended readings
- Secviz.org
- Vissec.org
- NvisionIP
  www.cert.org/flocon/2005/presentations/NVisionIPFlocon2005.pdf
- 14 ways to say nothing with visualization
  http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=299418
- 12 ways to fool the masses when giving performance results on parallel computers
  http://crd-legacy.lbl.gov/~dhbailey/dhbpapers/twelve-ways.pdf
- How not to lie with visualizations
  http://drona.csa.iisc.ernet.in/~vijayn/courses/DAV/papers/RogowitzTreinishHowNotToLieVis.p
- How to lie with statistics, Huff, 1954